Inside KECCAK

Joan Daemen

STMicroelectronics

(Joint work with Guido Bertoni, Michaël Peeters and Gilles Van Assche)

In our presentation we discuss the algebraic properties of the building blocks of KECCAK relevant in cryptanalysis and implementation. KECCAK is a sponge function family that makes use of an underlying set of fixed-length iterated permutations called KECCAK-f. The round function of KECCAK-f consists of 5 step mappings chosen for their ease of implementation and strong long-term diffusion and nonlinearity. We discuss the individual properties of these step mappings such as invertibility, translation-invariance and (when applicable) non-linearity, their interactions and the implications for resistance to attacks such as linear and differential cryptanalysis.

STMicroelectronics Belgium
joan.daemen@st.com